J. Korean Inst. Electr. Electron. Mater. Eng.
Vol. 37, No. 5, pp. 527-532 September 2024
doi: https://doi.org/10.4313/JKEM.2024.37.5.9
ISSN 1226-7945(Print), 2288-3258(Online)

Regular Paper

다중 공정변수를 활용한 저비용 PUF 보안 Chip의 제작

지홍석, 손 돌, 연주원, 길태현, 박효준, 윤의철, 이문권, 박준영

충북대학교 반도체공학부

Fabrication of Low-Cost Physically Unclonable Function (PUF) Chip Using Multiple Process Variables

Hong-Seock Jee, Dol Sohn, Ju-Won Yeon, Tae-Hyun Kil, Hyo-Jun Park, Eui-Cheol Yun, Moon-Kwon Lee, and Jun-Young Park

School of Semiconductor Engineering, Chungbuk National University, Cheongju 28644, Korea

(Received May 16, 2024; Revised May 28, 2024; Accepted May 31, 2024)

Abstract: Physically Unclonable Functions (PUFs) provide a high level of security for private keys using unique physical characteristics of hardware. However, fabricating PUF chips requires numerous semiconductor processes, leading to high costs, which limits their applications. In this work, we introduce a low-cost manufacturing method for PUF security chips. First, surface roughening through wet-etching is utilized to create random variables. Additionally, physical vapor deposition is added to further enhance randomness. After PUF chip fabrication, both Hamming distance (HD) and Hamming weight (HW) are extracted and compared to verify the fabricated chip. It is confirmed that the PUF chip using two different multiple process variables demonstrates superior uniqueness and uniformity compared to the PUF security chip fabricated using only a single process variable.

Keywords: Deposition, Low-cost, Physically unclonable functions (PUFs), Randomness, Surface roughness, Variations

1. 서 론

IoT (internet of things) 기술 및 이동통신의 발전으로 인하여, 다양한 중요 데이터가 가전, 차량, 모바일 기기, 그리고 데이터 센터에 저장되고 있다. 더불어, 저장되는 데이터의 종류 또한 단순한 개인정보에서 금융, 헬스케어 등으로 지속적으로 확장되고 있는 추세이다. 이에, 악성 소프트웨어에 의한 사이버 공격 위협 또한 꾸준히 증가하고 있으며, 보안 기술 도입의 필요성이 대두되고 있다 [1,2].

보안기술이란, 크게 소프트웨어 방식과 하드웨어 방식으로 분류된다. 소프트웨어 방식은 개인 키(private key)를 비휘발성 메모리(non-volatile memory) 내에 저장해 두기에, 온라인을 통한 업데이트가 용이하다. 하지만 메모리의 역설계(reverse engineering), 개인 키의 복제 및 변조에 취약하다는 한계가 존재한다. 이를 보완하고자, 최근 하드웨어 방식의 보안기술이 주목받고 있다. 이러한 보안기술의 주요한 특징은, 하드웨어가 지니고 있는 고유한 물리적 특성을 기반으로 하여, 개인 키를 보유한다는 사실이다. 따라서 하드웨어의 물리적인 분실이나 도난을 제외하면, 개인 키의 복제, 변조 또는 유출이 원천적으로 불가능하며, 사용 예로는, 신뢰 플랫폼 모듈(trusted platform module, TPM), 보안 토큰(hardware security module, HSM), 그리고 스마트 카드(IC 카드) 등 매체가 있다.

이와 같은 하드웨어 보안기술의 우수성으로 인하여, physically unclonable functions (PUF)이라는 보안기술에 대한 연구가 활발히 이루어지고 있다 [3-5]. PUF 보

✉ **Jun-Young Park; junyoung@cbnu.ac.kr**

안 chip은 양산 및 소형화 측면에서 매우 적합하다고 알려진 반도체 제조공정을 토대로 제작된다. 구체적으로, chip의 제조 공정에서 늘 존재하는 예측 불가능한 공정의 편차를 활용하며, 대표적인 예시로는, SRAM PUF [6], Via PUF [7], NAND flash PUF [8], nano-electromechanical systems (NEMS) PUF [9], surface roughness PUF [10] 등이 있다.

이러한 PUF 보안 chip은, 내부에 지닌 고유한 하드웨어 특성을 기반으로 생성된 개인 키를 보유하고 있기에, 개인 키의 역설계 및 복제가 불가능하다 [11]. 하지만 PUF 보안 chip의 제작은 표 1과 같이 다수의 반도체 제조 공정(deposition, etching 및 photo 등)을 필요로 하는 특성상, 여전히 높은 제조 비용을 요구하고 있다 [5,10]. 이에, PUF 보안 chip의 대중화를 위한 가장 중요 한 요소 중 하나는 제조 비용을 최소화하는 것이라고 할 수 있다.

본 연구에서는, 이러한 맥락에서 제조 비용 최소화를 위한 PUF 보안 chip 제조를 새로이 제안한다. 양산에 유리한 웨이퍼 기반의 공정을 유지하는 반면, 저비용의 식각 공정과 증착 공정만을 활용하고, 요구되는 제조 공정의 수를 가능한 최소화한다. 하지만 적은 공정 수로 인한 chip 보안성 저하를 보완하기 위하여, 다수의 반도체 공정변수(multiple process variables)를 업계 최초로 활용한다. 2개 이상의 공정 산포 조합을 통해, 우수한 PUF 보안 chip 제작이 가능하며, 제작된 chip의 보안성 검증을 위하여, hamming distance (HD) 및 hamming weight (HW) 분석법을 활용한다 [12].

2. 실험 방법

PUF 보안 chip 제작을 위하여, 4인치 p-type 실리콘 웨이퍼에 반도체 공정을 진행하였다. 먼저, 산화 공정(dry oxidation)을 활용하여, 300 nm 두께의 실리콘 산화막(SiO_2)을 형성하였다 [그림 1(a)]. 이후, buffered oxide etchant (BOE) 용액을 사용하여, 1분간 SiO_2 습식 식각 공정을 진행하여 다이싱을 진행한 시편의 표면 거칠기 심화를 유도하였다 [그림 1(b)]. BOE를 통한 실리콘 산화막 etching rate는 대략 105.6 nm/min으로 확인되었다. 그

Table 1. Expected number of fabrication processes to produce PUF chips.

Type of PUFs	Minimum number of depositions	Minimum number of etchings	Minimum number of photos	Number of random variables
SRAM PUF [6]	6 times	7 times	7 times	1
Via PUF [7]	6 times	2 times	1 time	
NAND flash PUF [8]	7 times	11 times	8 times	
Nano-electromechanical switch PUF [9]	3 times	5 times	3 times	
Surface roughness PUF [10]	2 times	2 times	1 time	
This work	1 time	1 time	-	2

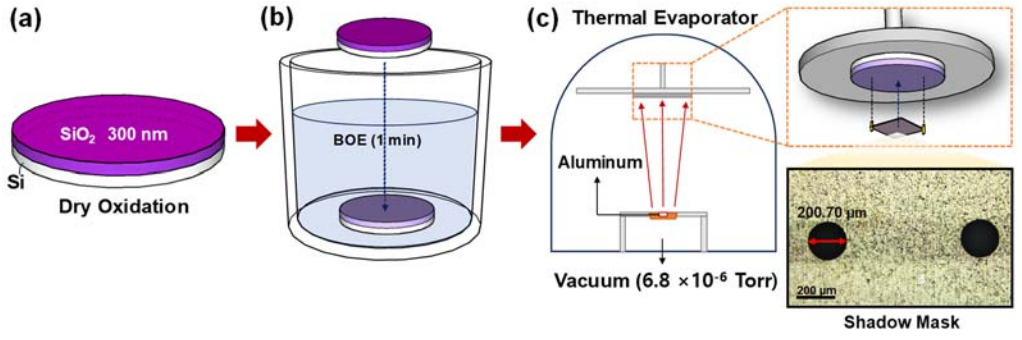

Fig. 1. Fabrication process flow of low-cost PUF chip using multiple process variables: (a) thermal oxidation using a furnace, (b) wet etching with BOE to increase surface roughness, and (c) Al deposition using a thermal evaporator for top electrode formation.

리고 그림 1(c)와 같이 silt diameter가 200 μm인 shadow mask를 웨이퍼에 부착하고, thermal evaporator를 활용하여 상부 금속 전극을 증착하였다. 공정 과정에서 사용된 thermal evaporator의 진공도는 6.8×10^{-6} Torr이며, 저비용인 금속인 동시에, 낮은 녹는점과 우수한 내식성을 가지고 있는 aluminum (Al)을 20 nm 두께로 증착하였다. 그리고 습식 식각 공정 적용 여부에 대한 PUF 보안 chip의 보안성 비교를 위하여, 습식 식각 공정만을 제외한 대조군을 별도로 제작하였다.

3. 결과 및 고찰

그림 2(a) 및 (b)는 각각 BOE를 통한 습식 식각 공정이 적용되지 않은 대조군(control group) PUF, 및 별도의 BOE 식각 공정이 적용된 실험군(experimental group) PUF의 단면 모식도 및 상부 광학현미경 이미지를 보여준다. 상부 금속 전극에서 명도가 높은 내경을 측정하였으며, 계측된 내경을 비교한 결과, 실험군과 대조군 모두 정규분포의 형태를 보여주었다. 다만, 실험군에서는 증가된 기판 표면 거칠기로 인하여, 명도 높은 부분의 크기는 감소하는 반면, 내경의 산포는 커지게 되었다. 다시 말해, 대조군 내경의 중간 값(M_d)의 크기는 191.4 μm인 반면, 실험군은 이보다 작은 137.4 μm으로 확인되었으며, 대조군의 standard deviation (σ)은 14.0인 반면, 실험군은 σ이 37.1로 기존 대비 165.0% 증가한 결과를 보여주었다 [그림 3(a) 및 (b)].

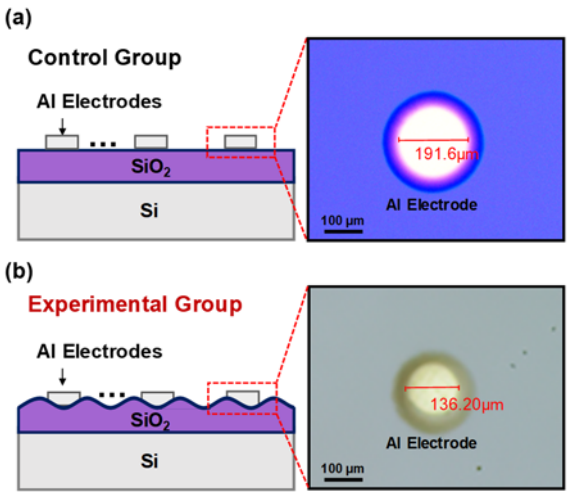

Fig. 2. Schematic and optical microscope images of fabricated PUF cells: (a) control group without etching using BOE and (b) experimental group after wet etching.

따라서 SiO_2 습식 식각 공정에 의해 증가된 웨이퍼 표면 거칠기는 PUF 보안 chip의 랜덤성(randomness) 강화에 기여 가능하다. 이러한 원리에 착안하여, 상부 금속 전극의 명도 높은 내경 값을 바탕으로, '0' 상태와 '1' 상태로 구분되는 이진 랜덤 변수를 생성하고, 이를 기반으로 물리적 보안 key를 구현하는 방식을 고안하였다. 먼저, 9개의 상부 금속 전극을 기준으로 하여, 3×3 Matrix 단위로 하나의 cell을 구성하였다. 이후, 계측된 모든 315개의 측정된 내경의 중간 값을 기준으로 하여, cell 내 중간 값보다 큰 상부 금속 전극의 수가 과반수인 경우를 '1'의 상태로, 과반수 미만인 경우를 '0'의 상태로 이진화한다. 이렇게 이진화된 cell의 상태를 바탕으로, 인접한 5개의 cell (총 45개의 상부 금속 전극)을 하나의 PUF 보안 key로 정의한다. 이와 같은 방식으로 총 7개의 PUF 기반의 물리적인 key가 제작된다 [그림 3(c)].

이후, 제작된 실험군 및 대조군 PUF 보안 chip을 대상으로, 보안성을 비교하였다. 이를 위하여, PUF 보안성을 분석함에 있어서, 널리 활용되고 있는 분석법인 haming distance (HD) 및 haming weight (HW)를 추출하였다 [12-14]. HD는 key의 유일성(uniqueness)을 검증하기 위한 파라미터로, 서로 다른 보안 key 간 서로 상이한 이진화 비트의 수를 의미하며, 이상적인 HD 값은 하나의 key를 구성하는 비트 수의 중간 값이다. 본 연구에서 제작되는 PUF 보안 chip을 구성하고 있는 각각의 key는 5개의 cell로 구성되어 있기에, 이상적인 HD 값은 2.5이며, σ 값은 작을수록 이상적이다 [10].

그림 4(a) 및 (b)는 그래프는 습식 식각 공정이 적용되지 않은 대조군과 습식 식각 공정이 적용된 실험군을 사용하여, 각각 PUF 보안 chip을 만들었을 때, 추출된 HD 값을 보여준다. 습식 식각 공정이 적용되지 않은 대조군 및 실험군에서는 이상 값인 2.5에 비교적 근사한 3.0과 2.0을 각각 보여주었다. 하지만 실험군의 경우 대조군에 비하여, 더 작은 σ을 보여주었다. 따라서 BOE를 활용한 표면 거칠기 증가가 반영된, 즉 다중 공정변수를 적용한 PUF 보안 chip이, 단일 공정변수를 적용한 PUF 보안 chip에 비하여, 유일성이 더 우수하다고 볼 수 있다.

HW는 각각의 key 내에서, 이진화 비트의 균일성(uniformity)을 검증하기 위한 파라미터이며, 한 개의 key 내부에 '0' 상태와 '1' 상태가 얼마나 균일한 비율로 분포하는지를 평가한다. 이상적인 HW 값은 하나의 key를 구성하는 총 비트 수의 중간 값인 2.5이다. 그림 5(a) 및 (b)는 실험군과 대조군의 HW 값을 보여준다. 습식 식각 공정을 적용한 실험군 PUF 보안 chip의 경우, HW 값이 3으로 대조군 값인 4보다 더 이상적인 값에 가깝다. 즉 BOE 식각

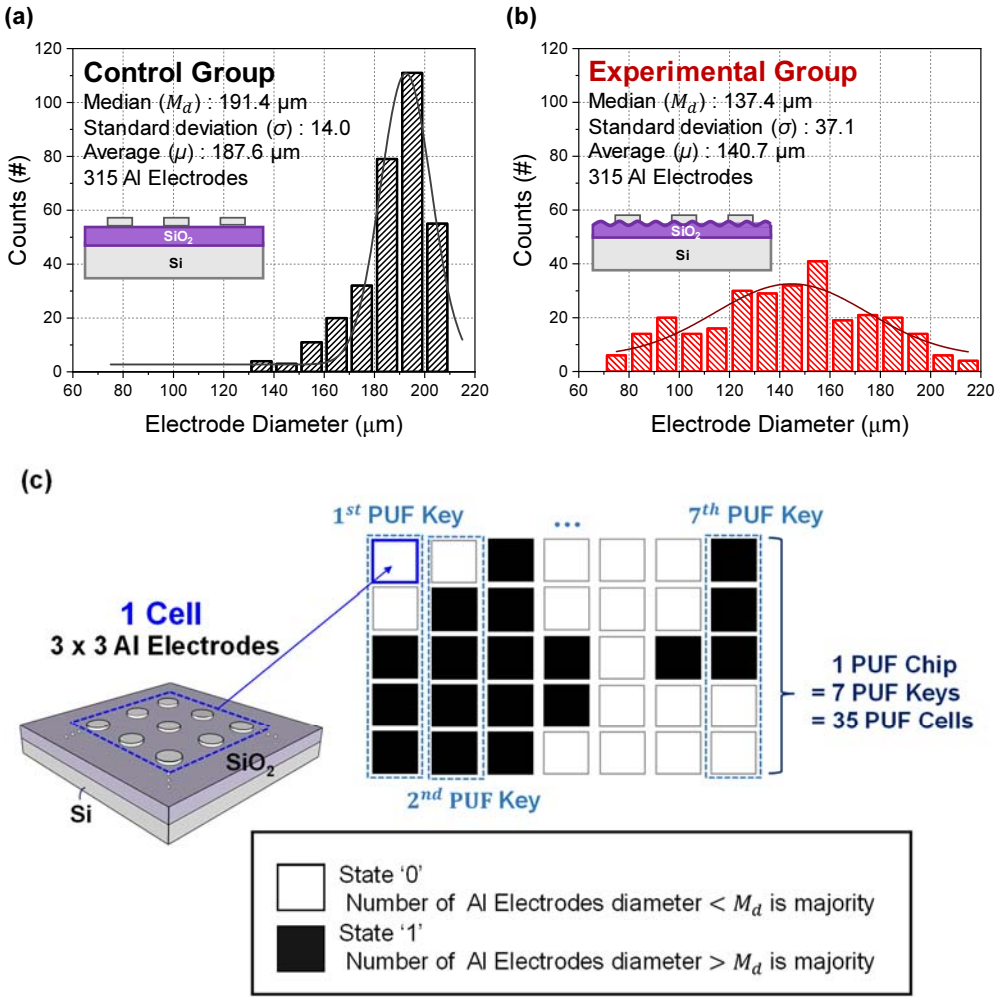

Fig. 3. Measured the diameters of Al electrodes of (a) the control group and (b) the experimental group. (c) Schematic of a PUF chip composed of 7 keys.

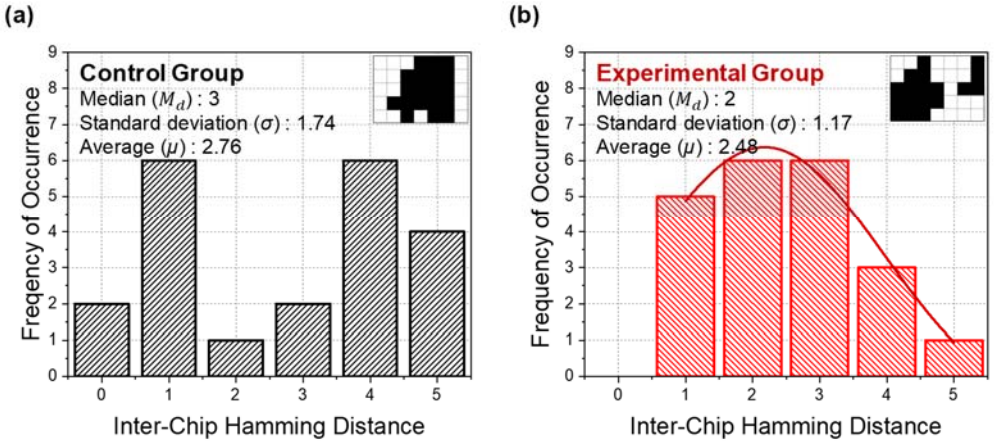

Fig. 4. Extracted hamming distance of the fabricated PUF chip to verify uniqueness: (a) control group and (b) experimental group.

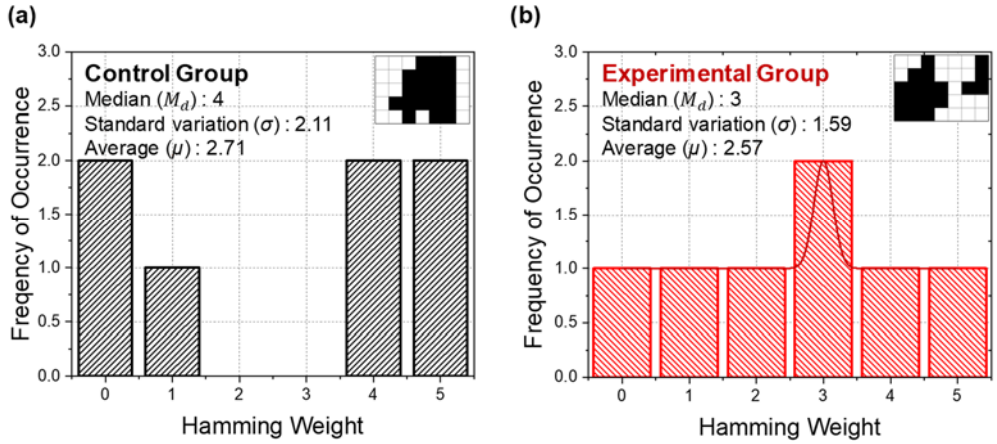

Fig. 5. Extracted hamming weight of the fabricated PUF chip to verify uniformity: (a) control group and (b) experimental group.

공정이 적용되어 표면 거칠기가 증가된 웨이퍼는 PUF 보안 chip의 균일성을 향상시킨다고 볼 수 있다. 결론적으로, 추출된 HD, HW 분석을 바탕으로 할 때, '증착 공정상의 산포' 그리고 '습식 식각 공정을 통한 표면 거칠기 산포'라는 두 가지의 다중 공정변수를 활용해 제작한 PUF 보안 chip은 '증착 공정상의 산포'라는 단일 공정변수만을 통해 제작한 PUF 보안 chip에 비해 유일성과, 균일성이 모두 우수함을 확인할 수 있다.

4. 결 론

본 연구에서는 저비용 PUF 보안 chip 및 제조 방법을 제안하였다. 이를 위하여, 실리콘 기판 및 thermal evaporator 반도체 공정을 활용하였다. 특히, 최소화된 공정 수로부터 기인할 수 있는 chip의 보안성 저하를 보완하기 위하여, 대기압에서 이루어지는 기판 습식 식각 공정을 추가하여, 기판의 표면 거칠기를 극대화하였다. 따라서 본 연구에서는 'PVD 증착 공정 산포' 그리고 '기판의 표면 거칠기 산포'라는 2개의 반도체 공정변수를 PUF 업계 최초로 적용하였다. Hamming distance (HD) 및 hamming weight (HW) 분석법을 활용하여, 다중 공정변수를 기반으로 제작된 PUF 보안 chip의 보안성은 단일 공정변수를 통해 제작 chip보다 더 우수함을 확인하였다. 이러한 연구 결과는, 높은 제조 비용을 지닌 기존의 하드웨어 기반 PUF 보안 chip의 응용처를 확장시키는 데 용이하다.

ORCID
Jun-Young Park https://orcid.org/0000-0003-4830-9739

감사의 글

본 과제(결과물)는 2024년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다 (2021RIS-001).

REFERENCES

[1] Y. Shah and S. Sengupta, *Proc. 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (IEEE, New York, USA, 2020) p. 406. doi: https://doi.org/10.1109/UEMCON51285.2020.9298138

[2] Y. Jin, *Electronics*, **4**, 763 (2015). doi: https://doi.org/10.3390/electronics4040763

[3] Y. Gao, S. F. Al-Sarawi, and D. Abbott, *Nat. Electron.*, **3**, 81 (2020). doi: https://doi.org/10.1038/s41928-020-0372-5

[4] S. Dotcenko, A. Vladyko, and I. Letenko, *Proc. 16th International Conference on Advanced Communication Technology* (IEEE, Pyeongchang, Korea (South), 2014) p. 167. doi: https://doi.org/10.1109/ICACT.2014.6778942

[5] B. Halak, M. Zwolinski, and M. S. Mispan, *Proc. 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS)* (IEEE, Abu Dhabi, United Arab Emirates, 2016) p. 137. doi: https://doi.org/10.1109/MWSCAS.2016.7870046

[6] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, *Proc. Cryptographic Hardware and Embedded Systems - CHES 2007* (Springer Berlin, Heidelberg, Vienna, Austria, 2007) p. 63. doi: https://doi.org/10.1007/978-3-540-74735-2

[7] T. W. Kim, B. D. Choi, and D. K Kim, *Electron. Lett.*, **50**, 876 (2014).

doi: https://doi.org/10.1049/el.2013.3474

[8] M. S. Kim, D. I. Moon, S. K. Yoo, S. H. Lee, and Y. K. Choi, *IEEE Trans. Nanotechnol.*, **14**, 384 (2015).
doi: https://doi.org/10.1109/TNANO.2015.2397956

[9] K. M. Hwang, J. Y. Park, H. Bae, S. W. Lee, C. K. Kim, M. Seo, H. Im, D. H. Kim, S. Y. Kim, G. B. Lee, and Y. K. Choi, *ACS Nano*, **11**, 12547 (2017).
doi: https://doi.org/10.1021/acsnano.7b06658

[10] D. H. Jung, J. M. Yu, J. Y. Ku, S. S. Yoon, J. H. Kim, J. K. Han, T. H. Kil, D. H. Wang, J. Y. Yeon, Y. K. Choi, and J. Y. Park, *IEEE Trans. Electron Devices*, **71**, 425 (2023).
doi: https://doi.org/10.1109/TED.2023.3338593

[11] C. W. O'Donnell, G. E. Suh, and S. Devadas, MIT CSAIL CSG Technical Memo 481 (2004).

[12] Y. S. Kang, M. K. Oh, S. J. Lee, and D. H. Choi, *J. Korea Inst. Inf. Secur. Cryptology*, **28**, 34 (2018).
https://public.thinkonweb.com/journals/kiisc/digital-library/15617

[13] P. H. Nguyen, D. P. Sahoo, R. S. Chakraborty, and D. Mukhopadhyay, *ACM Trans. Des. Autom. Electron. Syst.*, **22**, 1 (2016).
doi: https://doi.org/10.1145/2940326

[14] C. Bösch, J. Guajardo, A. R. Sadeghi, J. Shokrollahi, and P. Tuyls, *Proc. Cryptographic Hardware and Embedded Systems-CHES 2008* (Springer Berlin, Heidelberg, Washington, D.C., USA, 2008) p. 181.
doi: https://doi.org/10.1007/978-3-540-85053-3_12